An Efficient Control of Virus Propagation

Madihah Mohd Saudi
National ICT Security & Emergency Response Centre (NISER)
Malaysia
madihah@niser.org.my

Shaharudin Ismail
Islamic University College of Malaysia (KUIM)
Malaysia
shaharudin@admin.kuim.edu.my

Abstract – There are very few studies done in dealing with computer viruses in Malaysia. By realizing that, this research paper is done in managing of virus problem among ICT (Information Communication and Technology) users in Malaysia. Firstly, this research is establishing the existence of the problem through a questionnaire survey. This questionnaire survey was carried out at Malaysia specifically at Klang Valley and Putrajaya. Then a study was made on classifying virus, studying their symptoms and behaviour with the aim of controlling its propagation by studying their known features. The control is intended via a newly developed system which has been built applying Artificial Intelligent (Case-Based Reasoning) and Object Oriented Methodology. The ECOVP (Efficient Control of Virus Propagation) system that was developed is capable of educating users in handling computer virus incidents and at the same time helps to control computer virus propagation.

Introduction

Computer viruses have become real threats for computer users in the past few years. However, only few studies have been done trying to map out how large the problem actually is. In Malaysia, very few studies were done in dealing with computer viruses. The computer viruses problems in Malaysia caused big financial loss and it took an average of 1-2 months to eradicate virus and worm problems (Iman 2003; Saudi 2004). In the past, the distribution of anti-virus signature files required extensive periods of time to ensue (The Honeynet Project 2002) compared to the speed of spread of today's viruses and worms worldwide less than half of that time. This has raised the question of any other alternative ways in helping the society to reduce the loss of money especially when confronting with virus attacks? Currently, only few systems are capable of providing users step-by-step procedures in handling computer virus incidents. In order to handle a computer virus incident properly, the user awareness and education about computer viruses need an in-depth research (Kephart & White 2001; Perry 2002). A system that is capable to guide users on how to handle virus incidents following the incident response procedures need to be developed. These reasons give a sense of urgency for this study.

The questionnaire survey was conducted on the sampling population of Klang Valley and Putrajaya in Malaysia. The main aims of this questionnaire survey are to examine the computer viruses awareness among users in the sampling population, virus prevention levels in organizations and the impact computer viruses has caused and to produce a system, namely the Efficient Control of Virus Propagation (ECOVP) system, with a proper procedure in handling virus incident. The ECOVP system succeeded to overcome the weaknesses of the existing systems such as the Dynamic File Distribution System

(DFSD), Commercial Grade Immune System and Real-Time Virus Detection System (RVDS). The weaknesses of the existing systems and the solutions as well as the techniques provided by the ECOVP system are explained in the *Solution for Existing Systems* section.

The Problems

Several important aspects of computer viruses problem should be acknowledged and need an in-depth study in order to understand the problems. Hundreds of different computer viruses are written every day, and their numbers are increasing rapidly. Based on the observation and research done by others, below are the identified problems:

a. *User has no knowledge about computer viruses and having difficulties confronting virus incidents.*

   In article *Reducing "Human Factor" Mistakes*, Danchov reported human factors contributed to the security breach and dissemination of malicious code. Virus is one of the examples of the malicious code. In spite of the latest technological improvements, it was human or user, who plays roles in interacting and configuring devices or programs and contributing to the dissemination of malicious code. One of the approaches to overcome this problem is to increase the awareness level of the user (Lucas 2001), which is also one of the strategies in combating virus.

b. *Lack of research related with user education of computer viruses in Malaysia.*

   Most of the researches done in Malaysia are more focused using the Intrusion Detection System (IDS) techniques in solving virus problems (Keong 2003; Ramadass et al 2003; Sarim 2002; Zambri 2003). Nevertheless, there is still few research papers related to user education of computer viruses produced for the past 10 years in Malaysia (Fauzi 2003; Summers & Hussin 1991; Summers et al. 1992). This study is produced as a continuity of these researches and the urgency to produce more research related to user education of computer viruses in Malaysia.

c. *Need an efficient and an effective system that has standard operating procedure in handling computer viruses incident.*

   Many computer security programs and the standard operating procedures (SOP) in handling computer incidents are not effective and efficient especially when dealing with new and less understood class of computer threats (NIST 1992). Based on the Malaysia Computer Emergency Response Team (MyCERT) testing and also observations on report received from users (Saudi 2004), the eradication period for Code Red and Nimda was 3 months, Nachi and Sobig.F was 2 months and Blaster was 2 weeks. Why did it take 3 months, 2 months or 2 weeks to eradicate this worm? Can the eradication period shorten? More organizations are spending endless hours on repeating processes that are non-effective in completely eradicating the worm within the network due to uncoordinated efforts within the organization and non-

efficient ways of handling worm or virus incidents. In conjunction with a lack of standard operating procedures in handling worm or virus incidents, MyCERT is proposing to these organizations to form an operation center and follow the proposed standard operating procedures in handling computer worm or virus incidents (MyCERT 2002).

Questionnaire Survey

For the purpose of this study, the computer viruses awareness is defined and referred as having knowledge and understanding on how virus spread or also known as the channel of transmission for virus spread, the reaction and response that should be taken once infected with virus, the computer virus eradication procedure, the anti-virus functionality, capabilities and issues and the media channel of receiving the virus information. Meanwhile, the computer viruses impact is referred as the damage computer viruses have caused and how it affects user daily operation. The impact is similar to the payload of computer viruses. Viruses can do any kind of damage that software can do. This includes overwriting data, erasing files, scrambling system information, reformatting disks, disabling security systems or killing program processes. The other examples of the impacts caused by the computer virus are loss of data, loss of trust and reputation, information compromise, loss of customers, loss of loyalty and retention, loss of Web site, loss of time and loss of money.

Marko Helenius has conducted one questionnaire survey related to computer viruses in Finland (Helenius 1994). From his questionnaire survey result, the knowledge of viruses was quite poor in all sectors: government, local authorities and companies. Respondents' knowledge of viruses was best in government organizations. He did a large-scale questionnaire survey in Finland in the summer 1993. However, the macro viruses were non-existed then, so today the virus situation is a bit different. How important is virus prevention? The most positive attitude to virus prevention was in government organizations. 90 percent of the government organizations are using some kind of anti-virus program, 55 percent in local authority organizations and 60 percent in companies, respectively.

In year 2000, Love Bug virus had caused big impact all over the world. It attacked computers running Microsoft Outlook on Windows platform. It entered computers through e-mail messages. Once a message was opened, the virus was able to reproduce itself by finding address lists stored by the computer's owner and then sending itself to the addressees. If an addressee opened the attachment, a similar replication occurred, enabling the virus to spread rapidly. The virus was designed to steal Internet passwords and it was able to modify operating system files as well as certain sound and picture files residing in the infected computers. It had the effect of degrading network performance by inundating e-mail server systems and some web pages (Malphrus 2000).

In term of financial loss, in Malaysia the financial estimated loss to due Code Red and Nimda outbreak was RM21 million and RM31 million estimated lost due to Blaster and Nachi (Saudi 2004). In order to get information about computer viruses awareness among

users, prevention levels in organizations and the impact computer viruses have caused in Malaysia, a questionnaire survey was conducted on the sampling population of Klang Valley (which is referring to Selangor and Kuala Lumpur) and Putrajaya in Malaysia.

The objective of the questionnaire survey is to study and analyze the computer viruses awareness among users, the prevention levels in organizations and the impact computer viruses have caused in Klang Valley and Putrajaya. The sampling was chosen based on total subscribers of the Internet, location of the place for example located in urban area and as the federal government administrative and business centre in Malaysia. The Eight Malaysia Plan (2001 - 2005) shows that 53.6 percent of the total Internet subscribers are concentrated in the Klang Valley. Kuala Lumpur registers the highest penetration rate with 103.9 subscribers per 1000 people, followed by Selangor with 84.9 per thousand respectively. R. Ramachandran, NITC Secretariat held the disparity measure showed that these developed states; Kuala Lumpur and Selangor are above national level.

According to the paper presented by Dr. Narimah Ismail and Associate Prof. Dr. Musa Abu Hassan, Universiti Putra Malaysia; the study finding showed that there are differences in the level of readiness among respondents according to age, gender, income, rural-urban regions, and ethnic background. Overall it was found that respondents from urban areas are more ready to accept IT (with reference to the use of computer and the Internet) as compared to those in the rural areas. There was almost the same percentage of respondents from urban (88.4 percent) and rural (87.5 percent) areas in terms of having heard about the word IT (JARING Internet Magazine 2001). Putrajaya was chosen as the sampling population as it is the federal administrative centre of Malaysia. It is also located within the Multimedia Super Corridor (MSC) and it is set to be a model garden city with sophisticated information network based on multimedia technologies.

The Efficient Control of Virus Propagation (ECOVP) System

SANS Institute defined an incident as an adverse network event in an information system or network or the threat of the occurrence of such an event (SANS Institute 2003). In virus incident context for this research, the incident can be defined as threat of the occurrence made by the virus that could or results in a loss of data confidentiality, disruption of data and system integrity or financial loss. There are many factors that contribute to the virus incidents. One of the factors contributes to the virus incidents are when a virus is able to escape from antivirus or intrusion detection screen. When this occurs the virus will typically signal its presence, either as a direct result of its attempt to spread or as a side effect (Stone 2003).
Traditional security responses, such as risk analysis, contingency planning, and computer security reviews, have not been sufficient in controlling virus incidents and preventing significant damage (NIST 1992). Stories abound of virus incidents in which the problems grow worse or do not go away. Fearing unknown threats, some have misguidedly restricted their access to systems and networks. Consequently, some organizations spend far too much time reacting to recurring incidents at costs to convenience and productivity. A traditional computer security response typically is not prepared to detect and

subsequently react in a timely and efficient manner to computer security threats, such as virus outbreak, systems intrusions or serious bugs and vulnerabilities in systems.

Traditional computer security responses were designed to meet a threat scenario that considered incomplete or outdated today. Until the early 1980s, problems such as computer viruses and malicious hacking activities were not recognized as problems. Available guidance concentrated on subjects such as disaster recovery, physical security, backup contingency procedures, and data confidentiality. Organizations and users sometimes combined computer security responsibilities with general security responsibilities; therefore, those responsible for computer security often were not highly skilled in computer technology. For many years, this arrangement of resources sufficed (Wack 1991).

In conjunction with the problems arise, a system that is capable to help users handle virus incident efficiently and effectively using case based reasoning technique is produced as one of the strategies in handling virus incident structurally. Efficient refers to the way a system supports users in carrying out their tasks (Preece et al. 2002). A system can be very efficient at what it is doing but still not get to where it want to be because it is not doing the right things. That is where "effective" comes in. Effective means having the desired result (Markgraf 2004). Once the desired overall result is defined, the tasks leading to the result can be isolated and these tasks can then be completed efficiently. A system that is capable to help user handles virus incident efficiently and effectively meant that the system is capable to help and support user cleaning and managing virus problem correctly.

To ensure the system handles virus incident efficiently and effectively, accuracy testing and usability testing is carried out. Usability testing is a part of acceptance testing which is also known as Beta testing where it is targeted to end user. The usability testing tests if the system is capable to deliver it tasks efficiently and effectively to the users. Usability is a key concept in Human Computer Interaction (HCI) and it is concerned to make system effective to use, efficient to use, easy to learn and easy to use (Preece et al. 2002). As for Nielsen (Nielsen 1993) he defines usability as containing at least the learnability, efficiency and memorability, where learnability is referred as the system easy to learn, efficiency as system easy to use and memorability as the system easy to remember.

The ECOVP (Efficient Control of Virus Propagation) system is considered as capable to handle incident efficient and effectively when the end user is succeeded to clean up (eradicate) and do preventive measure to the infected machine. The accuracy of the ECOVP solution is very important for the end user to ensure the eradication and prevention procedure are carried out correctly. We put 100 percent as the expectation result for accuracy testing result. The accuracy benchmark would be based on the comparison with an anti-virus software scan result to the infected machine. The reason why researcher chosen 100 percent as the benchmark is from researcher point of view and experiences, when dealing with virus, solution given to the user must be 100 percent accurate. Even if one step is left out or not following the standard operating procedure it might lead to bigger damage or user might fail to do the eradication procedure. If the

result of the accuracy testing is less then 100 percent, we considered the ECOVP system is failed to achieve the system objective. As for the usability testing, the researcher put 80 percent as the expectation result or benchmark for usability testing which based on (Preece 2001) research. If the usability testing result is less then 80 percent, this indicates that the ECOVP system is not achieving its objective.

Why Need A System?

The ECOVP system is capable to educate user about computer viruses and helps to control computer virus propagation. The interactive system that is easy to use, easy to learn, easy to understand, efficient and effective are the principles used for the system design. The system consists of problem solving and guidelines on how to handle virus incidents. The solution provided based on the symptoms given by the user later will be diagnosed by the system using the case based reasoning technique. The user will rectify his machine based on solution recommended by the system. User succeeds in rectifying and following the instruction given by the system, helps to control the virus propagation. The existence of the ECOVP system also helps to minimize the damage caused by the viruses and user ICT usage is supported by this ECOVP system**.**

The users succeeded in identifying the seven main characteristics of the virus (the symptom, propagation mechanism, payload, virus type, operating algorithm, trigger mechanism and severity), which are used as the input to ECOVP system. The users also succeeded to clean up the virus in the infected machine based on solution given by the ECOVP system. The damages made by the viruses were succeeded cleaned by the user's shows that the existence of the ECOVP system is important as supportive system to help user in ICT usage.

The ECOVP System Design

Basically the ECOVP system consists of three (3) main features. The features are the Input Problem, System Engine and Output Solution. The system design diagram is displayed in figure 1 below.

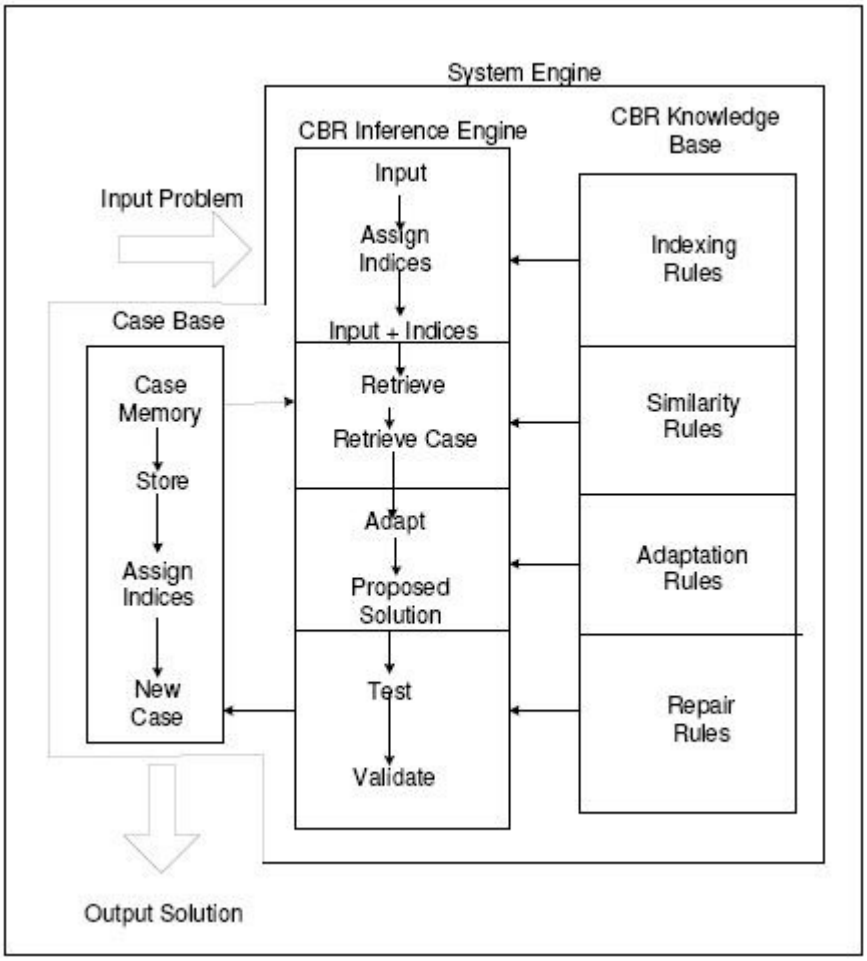

Figure 1

System Design for the ECOVP system

Input Problem

The Input Problem which is the input from user contributes to variety of solution where the solution consists of the prevention and eradication procedure. Basically the input problem is based on the ECOVP computer viruses classification. The input from a user which is also known as the problem consists of:

a. symptom
b. propagation
c. mechanism trigger
d. payload
e. severity
f. operating algorithm
g. virus type

The whole processes which starts with the input from the user and the solution as the output as illustrated is figure 2.

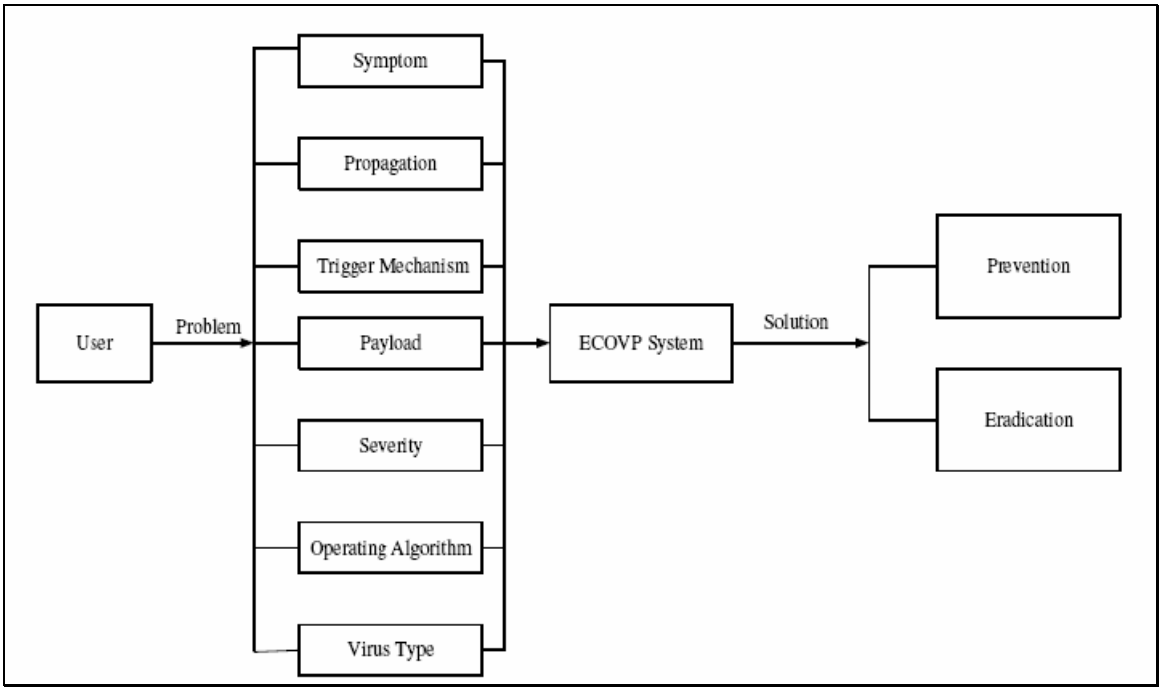

Figure 2

Input Problem and Output Solution

System Engine

System Engine of the ECOVP system consists of three (3) components as the following:

a. ***Case Base*** : It is the database of the cases.

b. ***Inference Engine***: Also known as the management of reasoning which consists of retrieves, reuse and revise processes.

c. ***Knowledge Base***: It is how the representation of the cases. Rules are assigned for each input.

Generally the rules of the Knowledge Base component are:

a. ***Indexing Rules****:*

It consists of assigning:
1. Indices ID for each GroupID, feature list and case.
2. Weight for GroupID
3. Numeric Value for feature list.

b. Similarity Rules

Using the nearest neighbour algorithm as the algorithm for similarity module, the target case Global Similarity value will be compared with other Global Similarity cases in the case base. The matching algorithm is based on the value of Global Similarity. Local Similarity is the total value of multiplication of the weight and the differences between target case and the existed cases in the case base for particular feature. The Global Similarity is the total of the entire local similarity feature. The equations for local similarity and the global similarity are:

$$\text{Local Similarity} = \sum_{i=1}^{n} W_i \times \text{sim}(f_i^I, f_i^R)$$

Where Wi is the weight of the particular feature and sim is the similarity function and fi^I and fi^R are the values for feature i in the input and retrieved cases respectively.

Global Similarity = Sum Total for all local similarity.

Later the global similarity is compared with the other 3 biggest global similarities that is existed in the case base. If the global similarity value is greater then the biggest global similarity value, the new global similarity becomes as the new biggest global similarity.

If user input the problem descriptor and the target case Global Similarity value is not
existed in the case base, he has to contact the Admin.

c. Adaptation Rules

The adaptation rule is to adapt a case to solve user problem. The system should gained experience every time when it is used to provide solution to present case. The system is capable to use the solution of previous case to solve the problem of present case where the previous case is similar to the present case. If the provided solution to the present case is suitable, the system should add this new case to the case base. With the increase cases of case base, the system will be able to provide more accurate cases to user. A case consists of two parts which are the problem and the solution. For a new case that will be added to the case base by the user, the first part of new case is copy from the present case and the second part is copy from the matched case. The new case is the combination of previous case and present case.

d. Repair rule

The virus expert will review the cases in the case base to ensure the solution provided is right. If the solution is not correct and not satisfied, the virus

expert will amend the solution. The amendment version later is saved in the case base which would overwrite the old solution.

Output Solution

This component will display the solution to the user. A solution consists of the prevention procedure and eradication procedure. As illustrated in figure 4.3, the solution is consists of the prevention and eradication procedure. The solution is also part of the domain knowledge. This solution features are derived from the questionnaire survey result analysis. Based on the questionnaire conducted, most of the user interested to know the prevention and the eradication procedure when confronting the virus incident. The prevention and eradication for this system is defines as:

a. ***Prevention***: This procedure is to avoid and prevent the virus from the entire system completely.
b. ***Eradication***: This procedure is to remove the virus from the entire system completely.

The solution given in this system is based on the solution provided in anti virus advisories, computer viruses book and MyCERT advisories (www.mycert.org.my). The anti virus advisories are from the Symantec anti virus (www.symantec.com), Trend Micro antivirus (www.trendmicro.com) and F-Secure anti virus (www.f-secure.com).

The solution of the ECOVP system is controlled by the different type of virus. There are three main types of viruses as shown in Figure 4. Boot sector infectors attach themselves to the boot sector of hard or floppy disks containing the computer's start-up instructions. These viruses overwrite the original boot sector instructions so that they take immediate control. They tend to create bad sectors on the disk where they store the rest of their program code. System infectors attach themselves to various part of the computer's operating system or master control program software. The virus may infect the input or output section of the operating system coding, the command interpreter or any other system file. They gain control of a system before virus detection or prevention program can get into the memory to do its job. Application infectors can affect any applications program. These viruses may or may not be memory resident and may infect every time a new program is loaded or a program is copied from one disk to another.

These three main types of the virus are later categorized into eight types because this virus type will vary the solution of the system. The eight types are shown in Figure 4. Table 1 shows example how the three different solutions are produced although the user selects the same symptom.

Table 1

Variety of Solution

Virus Type	Symptom	Solution
Boot Sector	Computer shutdown automatically	**Prevention**: Disable start boot up computer from external device. **Eradication**: Boot up from clean floppy disk.
Application	Computer shutdown automatically	**Prevention**: Disable the active scripting and the auto executable command. **Eradication**: Make sure to patch the application with the latest patch.
System	Computer shutdown automatically	**Prevention**: Always patch the OS with the latest patch by clicking the Windows Update. **Eradication**: Patch the OS with the latest patch.

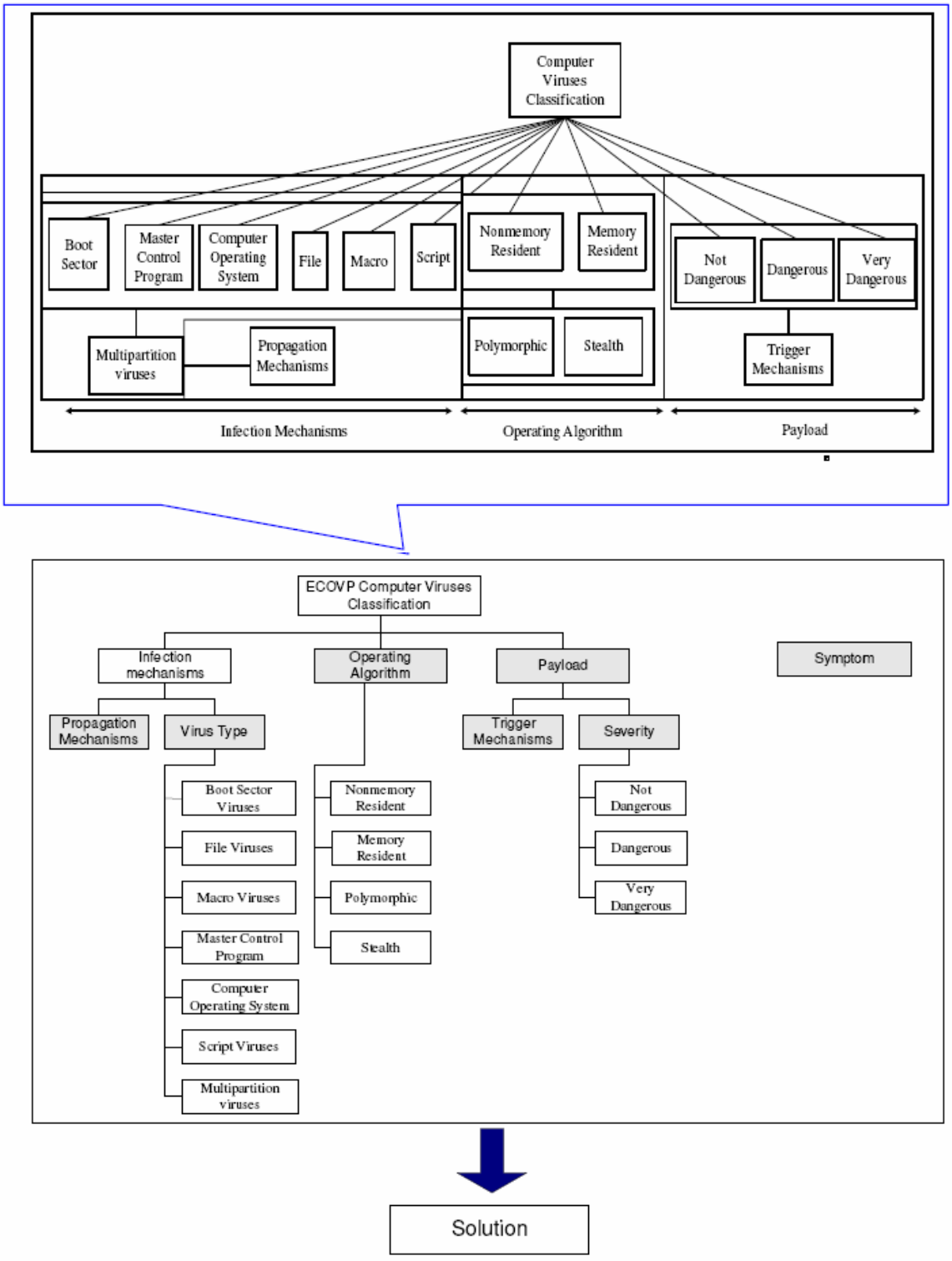

Figure 3

Problem Derivation Features

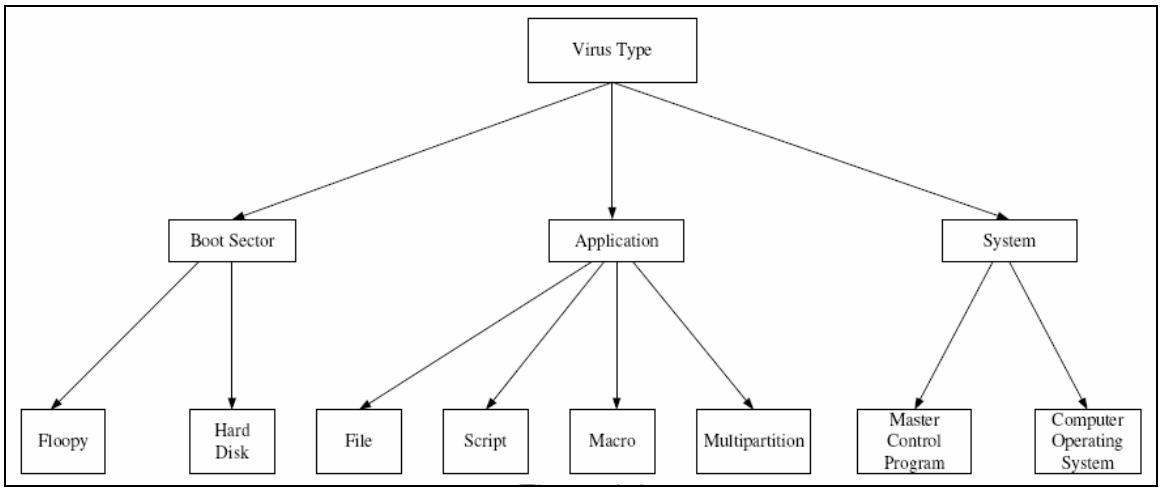

Figure 4

Virus Type Structure

Solution for Existing Systems

Based on the analysis made to the three existing systems, namely the Dynamic File Distribution System (DFSD), Commercial Grade Immune System and Real-Time Virus Detection System (RVDS), four weaknesses or problems of these systems have been identified. The ECOVP system succeeded to overcome the above weaknesses and provide solutions and techniques.

Problem 1:

There is a need to produce a system which is capable in helping end-user managing and handling virus incident in a more effectively and efficiently way. The solution provided by the system to end-user must be accurate**.**

Solution for Problem 1:

The ECOVP system has the capability to handle incident efficiently and effectively, which allows the end-user to clean up (eradicate) and do preventive measure to the infected machine. From the accuracy testing carried out in the studies, from 230 cases used by the testers to eradicate and do preventive measure 100% of the solutions given by ECOVP system were accurate. This accuracy referred to a solution whereby the end-user had succeeded in cleaning up or eradicated and carried out a preventive measure to the infected machine**.** Later, the AVG anti-virus was used to scan the infected machine to ensure that the machine was virus free. When the AVG anti-virus software was used to scan the infected machine, no virus was found. Thus, it can be concluded that this was due to the accurate solution given by the ECOVP system. With the accurate testing result, the ECOVP system has fulfilled one of the criteria that should be fulfilled by the ECOVP system in order for the system to be categorized as a system capable to help user handles virus incident efficiently and effectively.

Problem 2:

The solution provided by the system to end-user must follow the standard operating procedure. When dealing with viruses, following the right procedure is a must to ensure that end user succeed in performing eradication and prevention procedure to the infected machine.

Solution for Problem 2:

The ECOVP system solution consists both of prevention and eradication procedure in handling virus problem. The eradication procedure was built based on the Malaysia Computer Emergency Response Team (MyCERT) standard operating procedure. MyCERT had produced a complete guide on Computer Worm Handling - Standard Operating Procedure (SOP), offering a proper mechanism to assist and guide users and organizations to eradicate virus or worm outbreaks. Today, many organizations and individual users fail to remove the viruses thoroughly. This is due to the major reason - lack of a proper methodology in controlling and eradicating the viruses.

Based on researchers made, following MyCERT standard operating procedure helped to eradicate the virus problem. This procedure has been implemented and tested in many organizations such as government agencies, local and private universities and corporate organizations and the result was very satisfying. Viruses and worm were successfully eradicated and removed from their organizations. Thus, when dealing with viruses, following the right procedure is a must. This is one of the main features that made ECOVP system different from any other systems in handling virus problem.

Problem 3:

A system that is user-friendly especially to non-technical person.

Solution for Problem 3:

In this project, the researcher produces a system to assist end-users in responding to virus incident. The ECOVP system has documented procedures on how to eradicate and prevent virus incident. The ECOVP system assisted end users in performing analysis of the incident by providing problem descriptor form where user needs to identify seven main features of the virus, which are the symptom, propagation mechanism, trigger mechanism, payload, severity, operating algorithm and virus type. Even though the term used to describe this worm was new to end user, the tooltip text in the ECOVP system helps end user to understand each term used by the system. By moving the mouse or cursor on the virus term, an explanation of such term will automatically be explained in a simple English language to ensure easy understanding especially for the non-technical people. Option list is provided offering user an easy answer.

Based on acceptance survey, majority (87%) of the respondents strongly agreed that ECOVP is easy to use and majority (80%) approved that the explanation for problem

descriptor and solution form was clear and easy to understand. Thus it can be concluded that end user faced no problem regarding the virus term used in the ECOVP system. This acceptance survey was carried out in Klang Valley and Putrajaya involving 115 users from different background, age, education level and occupation. Ninety six percent (96%) of them were from non-technical background but all succeeded to eradicate and did preventive measure on the infected machine. Ninety (90%) of the testers strongly agreed that the ECOVP system had helped them in solving virus problem. ECOVP system guides a non-expert through a well-defined analysis process until the eradication and prevention stage. The current situation, requiring an expert using primitive tools to proceed through some ad-hoc process, does not scale and is difficult to reproduce, teach or improve.

Providing some automated guidance in the form of a software tool such as ECOVP system would allow process improvement, better education and distribution of the collective knowledge base of security experts. In ECOVP system, the end users play roles as the incident analyst as well as the virus analyst.

Problem 4:

To consider building a system that does not need a regular update of signature file.

Solution for Problem 4:

ECOVP system is using the case based reasoning technique where the solution given is based on the problem description given by the end users. If the solution is not found in the system, the system will then search for a similar case to be matched to the solution. No specific update in the anti-virus system is required.

The Advantages of ECOVP System

1. User Friendly Interfaces

Properly arranged of command buttons and drop down list menus are provided for the users to easy select. The time to learn about the system is minimized due to its simple layout and flow. There is also a message, which describes each label for problem descriptor by moving the mouse to the problem descriptor label.

2. CBR Technique to Generate Solution

By using the CBR (case based reasoning) technique, the system is capable to provide a most similar case to the presented problem as a solution. If the retrieved case is not suitable to be the solution due to the similarity between cases is not determined accurately, the administrator can adjust the numeric value of each problem descriptor.

3. Expandable Case Base

The system has ability to add new case to the case base. Every time when the user is using the system, the system will retrieved three most similar cases as the solution. The user is then allowed to choose the most suitable case to be added to the case base. Therefore, with the increasing cases in the case base, the variety of solution get to increase too and the ability of the system will be improved in order to provide more accurate case as solution to the user.

System Limitations

1. Limited Scope of Domain Knowledge

For this system the domain knowledge is only limited to computer viruses on Windows platform.

2. Stand Alone System

This system is a stand-alone system and cannot be accessed online.

3. Average users are unfamiliar about technical aspects of viruses

In order for the user to use this system, the user must be capable to understand the technical aspect of the viruses. The seven main features of virus which are the symptom, propagation mechanism, payload, virus type, operating algorithm, trigger mechanism and severity that needs to be identified by the user must be clearly understood by the end user. Any misunderstanding will cause user to face problems later on.

To overcome this problem, the system was developed by using the usability design principle which in under the Human Computer Interaction (HCI) field. Usability is a key concept in HCI and it is meant to make the system effective, efficient and easy to use as well as easy to learn (Preece et al. 2002). Nielsen (Nielsen 1993) defines usability as containing at least the learnability, efficiency and memorability, where learnability is referred as the being easy to learn, efficiency as easy to use and memorability as easy to remember. As for ECOVP system, the approach used to overcome this problem is by using the tooltip text tool where each term of the virus used is explained in simple plain English for easier understanding, memorizing and easy to use. Users just have to move their cursor on each term to display the definition for each term used in the ECOVP system. The option list for each problem descriptor provided in the ECOVP make it easier to use. Based on acceptance testing carried out, eighty percent (80%) of testers strongly agreed that they could understand and act on the information provided by this software. The option list for each problem descriptor made their selection easier and the explanation for solution form is clear and easy to understand.

Future Enhancement

Even though the ECOVP system is one of the ways to help user handles virus incident efficiently and effectively, there is always room for enhancement and other solution for this problem. Some of the enhancements proposed are:-

1. Use Bigger Scope of Domain Knowledge

For future work, the domain knowledge would include the computer viruses, worms and Trojan horses on all platforms.

2. System to Be Online

To make the system easy to be maintained and accessible from anywhere and anytime, the future work would involve implementing the system online.

3. Interfaces to Be More Interactive and Attractive

To make the interfaces more interactive and attractive, the future work would involve implementing system agent and integrating the human computer interface concept. The existence of the system agent will make the system more interactive and easier to use. To do this, the human computer interface concepts, which involve choosing the right color for the interfaces, the location of the command button and the label and anything related with the interfaces, will be studied in more depth for future implementation.

4. Use My SQL as the Database

To enable the system to keep more data and retrieve them in a faster mode, the My SQL is recommended to be used in the system. If the total features are increased as well as the scope of domain knowledge, the result is the total of cases in case bases will definitely become immense. The My SQL provides higher ability to store the cases and it is more efficient to handle huge database.

5. To Produce Automated Generated Statistic for the Match Cases

To check and retrieve match cases for the system in faster mode, the future work would involve producing the automated generated statistic for the match cases.

6. To Integrate the Malicious Code Analysis Steps

For this system, the technique use to detect, analyze and remove computer viruses is targeted for non-technical person. For future work, the same technique will become more technical and targeted to computer professionals who work in a computing environment where viruses are widespread. This would include the methodology to analyze the malicious source code manually or using the tools.

7. To use visualization technique to explain virus technical term

One of the ways to make each of virus term more interesting and easier to be understood is by using the visualization technique. Visualization provides visual depictions of very large information spaces. Humans are highly attuned to images and visual information (Tufte 1983). Pictures and graphics can be captivating and appealing, especially if well designed.
A visual representation can communicate some kinds of information much more rapidly and effectively than any other method.

Conclusion

The questionnaire result and analysis provides the current situation of the computer viruses awareness, virus prevention levels in organizations and the damage computer viruses have caused in Klang Valley and Putrajaya. The result from the questionnaire survey showed that the users had a good knowledge related with the eradication procedure, anti-virus functionalities and capabilities and used the information received related with viruses to equip themselves with the latest information of viruses and they were prepared in confronting the viruses spread. The prevention level for organization was very good but users were not satisfied with the virus protection and viruses had a big impact to them where one of the major impacts was they were unable to perform their daily work. Even though the level of the user awareness and virus protection is very good, that does not mean the eradication and prevention procedure taken by the user are efficient and effective.

The ECOVP (Efficient Control of Virus Propagation) system is considered as capable to handle incident efficient and effectively when the end user is succeeded to clean up (eradicate) and do preventive measure to the infected machine. The ECOVP system also succeeded to overcome four weaknesses or problems identified in the other three existing systems, namely the Dynamic File Distribution System (DFSD), Commercial Grade Immune System and Real-Time Virus Detection System (RVDS). ECOVP system is also capable to educate user about computer viruses and helps to control computer virus propagation.

References

"Establishing A Computer Security Incident Response Capability, Computer Systems Laboratory Bulletin: Advising users on Computer Systems Technology," *National Institute of Standards and Technology (NIST),* February 1992, (Online Posting) http://csrc.nist.gov/publications/nistbul/csl92-02.txt [Viewed 17/03/2005].

Fauzi, S.S.M. *A Study On Computer Viruses Attacks And The Way To Cure Them*, Degree Thesis, Faculty Information System Engineering, UiTM, Malaysia, October 2003.

Helenius, M. *Computer Viruses in Finland - A Questionnaire Survey*, Master Thesis of Sciences, University of Tampere, 1994.

Iman, M.R.M. "Negara Rugi RM31 Juta Serangan Terbaru Virus Komputer*," Utusan Malaysia,* 29 August 2003, (Online Posting) http://www.niser.org.my/news/2003_08_29_01.html [Viewed 17/03/2005].

Keong, C. *Analysis and Design of Intrusion Detection SystemImplementation,* Dissertation (M.Sc.Comp), Fakulti Sains Komputer dan Teknologi Maklumat, Universiti Malaya, Malaysia, 2003.

Kephart, J. and White, S. "How Prevalent are Computer Viruses?" (Online Posting) http://www.research.ibm.com/antivirus/SciPapers/Kephart/DPMA92/dpma92.html [Viewed 17/03/2005].

Lucas, J. "The Malicious Logic Battle: Understanding the Enemy," *An Enterasys Networks Whitepaper*, October 2001, (Online Posting) http://www.enterasys.com/products/whitepapers/9012849.pdf [Viewed 17/03/2005].

"MA-041.052002: Computer Worm Incident Handling Standard Operating Procedure," *Malaysia Computer Emergency Response Team (MyCERT),* 2 May 2002, (Online Posting) http://www.mycert.org.my/advisory/MA-041.052002.html [Viewed 27/10/2004].

"Malaysian Readiness Towards K-Society, A Statistic Measurement*," JARING Internet Magazine*, August 2001.

Malphrus, S.R. "The "I Love You" Computer Virus and the Financial Services Industry," 2000, (Online Posting) http://www.federalreserve.gov/boarddocs/testimony/2000/20000518.htm [Viewed 22/08/2005].

Markgraf, B. "Efficient and Effective," 23 September 2004, (Online Posting) http://www.suite101.com/article.cfm/small_business/111086 [Viewed 17/03/2005].

Nielsen, J. "Usability Engineerin," *Academic Press*, USA, 1993, pp.115-163.

Perry, D. “The future of viruses”, *PC Answers*, Issue 108, July 2002. (Online Posting) http://www.pcanswers.co.uk/tutorials/default.asp?pagetypeid=2&articleid=7929&subsectionid=607 [Viewed 17/03/2005].

Preece, J., Rogers, Y. and Sharp, H. *Interaction Design: Beyond Human Computer Interaction*, John Wiley & Sons, New York, 2002, pp.14.

Ramadass, S., Osman, A.B., Budiarto, R., Sathiananthan, N., Keong, N.C. and Jong, C.S. “Real-Time Virus Detection System Using iNetmon Engine,” *APAN/PRAGMA 2003 Conference in Fukuoka,* Network Research Group, School Of Computer Science, University Science Malaysia, 2003, (Online Posting) http://www.qgpop.net/2003fukuoka/papers/B6-1.doc [Viewed 17/03/2005].

“SANS Glossary of Terms Used in Security and Intrusion Detection,” *SANS Institute,* May 2003, (Online Posting) (Available from: http://www.sans.org/resources/glossary.php#I [Viewed 22/08/2005].

Sarim, H.M. *The Effectiveness of Detection Methods in IntrusionDetection Systems,* Dissertation (M.Comp.Sc.), Fakulti Sains Komputer dan Teknologi Maklumat, Universiti Malaya, 2002.

Saudi, M.M. “Situational Report on Major Worms Outbreaks Up to Year 2003 in Malaysia,” 2004, (Online Posting) http://www.mycert.org.my/other_resources/NISER-MYC-PAP-7070-1.pdf [Viewed 17/03/2005].

Stone, J. “Detecting and Recovering From a Virus Incident,” 2003, (Online Posting) http://www.symantec.com/symadvantage/019/recover.html [Viewed 22/08/2005].

Summers, W.C. and Hussin, N.M. “Computer Viruses and Practicing Safe Computing,” in *Proceedings of EDUCOMP '91, National Symposium on Educational Computing*, Kuala Lumpur, Malaysia, November 1991.

Summers, W.C., Ibrahim, Z. and Hussin, N.M. *Computer Viruses: What They Are and How to Prevent Them,* Federal Publications, Kuala Lumpur, September 1992.

“The Reverse Challenge,” *The Honeynet Project,* (Online Posting) http://www.honeynet.org/reverse/ [Viewed 17/03/2005].

Tufte, E. *The Visual Display of Quantitative Information*, Graphics Press, Chelshire, CT, 1983.

Wack J.P. “Establishing a Computer Security Incident Response Capability,” *Computer Systems Laboratory National Institute of Standards and Technology (NIST) Special Publication 800-3,* November 1991, (Online Posting) http://downloads.securityfocus.com/library/estcsirc.ps. [Viewed 17/03/2005].

Zambri, M. *Evaluating Intrusion Detection Systems in a Unix Based Environment,* Master Dissertation of Software Engineering, Fakulti Sains Komputer dan Teknologi Maklumat, Universiti Malaya, 2003.